CS-1S(I)
(3-20-2002)

DRAFT

U.S. DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. CENSUS BUREAU
Acting as Collecting Agent For
BUREAU OF JUSTICE STATISTICS
U.S. DEPARTMENT OF JUSTICE

2001 COMPUTER SECURITY SURVEY INSTRUCTIONS

Introduction

This manual provides instructions to assist you in completing the Computer Security Survey questionnaire. **Part A** provides the general instructions. **Part B** provides question-specific instructions for reporting in the Computer Security Survey.

Purpose of the Survey

The purpose of this survey is to collect information about the nature and extent of computer security incidents experienced by businesses located in the U.S. The data you report will provide first-time information on the impact of computer crime on businesses. Specifically, data from the Computer Security Survey will provide information on the frequency and types of computer crime, the cost of computer security, and the economic losses sustained due to computer crime.

Legal Authority and Confidentiality of Data

Your participation in this survey is voluntary. We are conducting this survey under the authority of Title 13, United States Code, Section 182. By Section 9 of the same law, your report to the Census Bureau is confidential. It may be seen only by persons sworn to uphold the confidentiality of Census Bureau information and may be used only for statistical purposes. Further, the information you provide is immune from legal process.

Burden Hour Estimate

Public reporting burden for this collection of information is estimated to average 60 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Paperwork Project 0607-0725, Room 3110, Federal Building 3, U.S. Census Bureau, Washington, DC 20233-1500. You may e-mail comments to Paperwork@census.gov; use "Paperwork Project 0607-0725" as the subject.

PLEASE INCLUDE THE FORM NAME AND NUMBER IN ALL CORRESPONDENCE. Respondents are not required to respond to any information collection unless it displays a valid approval number from the Office of Management and Budget. This 8-digit number appears in the top right corner on the front of the Computer Security Survey questionnaires.

Part A – GENERAL INSTRUCTIONS

Survey Scope – This survey collects computer security data for nonfarm companies, organizations, and associations operating within the United States. Information for agricultural production operations should be excluded. However, companies performing agricultural services are included. **Information for churches, nonprofit organizations, and organizations that are government owned but privately operated should be included.**

Reporting Entity – Report computer security data for all domestic operations of your enterprise, including subsidiaries and divisions. For this report, the terms enterprise and company are used interchangeably. An enterprise is a business, service, or membership organization consisting of one or more establishments under common ownership or control. It includes all establishments of subsidiary companies, where there is more than 50 percent ownership, as well as establishments of firms which the enterprise has the power to direct or cause the direction of management and policies. **Holding companies should report for the entire corporation, including all subsidiaries under their ownership.**If you are unable to consolidate records for the entire company or have reporting questions, please call **1–800–227–1735.** For purposes of this survey exclude data for Puerto Rico, the Virgin Islands, and U.S. Territories.

Survey Period – Report data for calendar year 2001. If calendar year figures are not available, reasonable estimates are acceptable. If you cannot provide data on a calendar year basis, fiscal year data are acceptable. If fiscal year data are used and your fiscal period ends in January, February, or March, report for the fiscal year ending in 2002. Otherwise, report for the fiscal year ending in 2001. Indicate in Question 20, Reporting Period, the exact dates the data represent if they are not for the calendar year.

Estimates are acceptable – The data requested on this report form may not correspond to your company's accounting records. If you cannot answer a question from your company records, please provide carefully prepared estimates. For questions requiring dollar amounts, if your company had none to report for the 2001 reporting period, enter "0" in the appropriate cell(s).

Part A – Continued

Company Ceased its Operation or Was Sold –

a. If your enterprise ceased its operation during the period covered by this report, complete the form for the period of time the company was in operation. Also, indicate in Question 21, Operational Status, the company's status and the date the company ceased its operation.

b. If your enterprise was sold during the period covered by this report, complete the form for the period of time the enterprise was in operation prior to the acquisition. Indicate in Question 21, Operational Status, the company's status, the date the acquisition became effective, and the name and address of the successor company.

Additional Forms – Photocopies of this form, are acceptable. If you require additional forms, contact us at the toll-free number, email address or business address provided at the bottom of this page. In written correspondence, please include the 11-digit identification number from the questionnaire's address area.

Filing the Report Form – Return your completed form in the preaddressed envelope. If you are not using the pre-addressed envelope, return it to the address below or fax it to 1–888–353–4102. Make a copy of the completed questionnaire for your company records.

U.S. Census Bureau
1201 East 10th Street
Jeffersonville, IN 47132-0001

Filing Extensions – If you cannot complete the survey by the due date shown in the upper left corner on the cover of the form, you may request an extension of time by calling the toll-free number, sending an e-mail to the internet address, or writing to the business address provided below. In written correspondence, please include the 11-digit identification number located in the questionnaire's address area.

Direct any **QUESTIONS** regarding this form to:

U.S. Census Bureau
Computer Security Survey Processing
ATTN: Business Investment Branch,
Company Statistics Division, Room 1285-3
Washington, DC 20233-6400

Toll-free Number: 1-800-227-1735
FAX Number: 1-888-353-4102
E-mail: csd@census.gov

Part B – INSTRUCTIONS BY QUESTION

Section 1 – COMPUTER SECURITY CONCERNS

Question 1 – What are the top three computer security concerns for this company?

Mark (X) the company's top three computer security concerns from the following categories:

1. **Embezzlement –** Computer-related crimes involving the misappropriation of something of value by a person to whom it was entrusted.

2. **Fraud –** Computer-related crimes involving the deliberate misrepresentation or alteration of data or documents in order to obtain something of value.

3. **Forgery or theft of proprietary information –** The copying, alteration, imitation or theft of computerized documents with the intent to use them fraudulently or for some other purpose for which they were not intended. Examples of computerized documents include client information, trade secrets, graphics copyrighted material, data, forms, files, lists, personal or financial information, etc.

4. **Denial of service –** The prevention of authorized access to a system resource or the delaying of system operations and functions. For example, the loss of e-mail service, the temporary loss of all network connectivity and services, or the loss of e-commerce.

5. **Vandalism or sabotage –** The malicious alteration, damage or destruction of computer files, data, programs, software, Web pages, etc.

6. **Computer virus –** A section of computer code using malicious logic, that propagates by infection. For example the virus inserts a copy of itself into and becomes part of another program.

7. **Other intrusion or breach of computer system –** Other penetration or attempted penetration of the company's computer system which does not result in any of the incidents listed above. For example, hacking or sniffing.

8. **Misuse of computers by employees (Internet, e-mail, etc.) –** The improper use of company computer resources by employees such as using the company's computer resources for personal gain, sending personal or improper e-mail, abusing Internet privileges, loading unlicensed software, etc.

9. **Unlicensed copying or use of software –** The unauthorized copying or use of software which the company developed or for which it holds the copyright. Classify unauthorized copying or use of other software by employees under "Misuse by employees," above.

Section II – COMPUTER INFRASTRUCTURE AND SECURITY

Question 2a – In 2001, what types of computer networks did this company use?

Mark (X) the types of computer networks the company used in 2001 from the following categories:

1. **Local area network (LAN) –** A computer network that spans a small area such as a single building or group of buildings.
2. **Wide area network (WAN) –** A computer network that spans a large geographical area. Usually a WAN consists of two or more local-area networks (LANs).
3. **Process control network –** A network with an automated control of a process, such as a manufacturing process or assembly line. It is used extensively in industrial operations, such as oil refining, chemical processing and electrical generation. It uses analog devices to monitor real-world signals and digital computers to do the analysis and controlling. It makes extensive use of analog/digital, digital/analog conversion.
4. **Virtual/private network (VPN) –** A network that is constructed by using public wires to connect nodes. For example, systems that allow you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network.
5. **Electronic data interchange (EDI) –** An Electronic Data Interchange (EDI) is a proprietary electronic system used for exchanging business data over a computer network.
6. **Internet access –** Access to inter-connected networks connecting millions of computers globally. Users can access information and applications from other computers and communicate with other users.
7. **Intranet –** An internal network similar to the Internet but surrounded by a firewall to prevent access from users outside the company, organization, or facility.
8. **Extranet –** A network that uses Internet/Intranet technology to make information available to authorized outsiders. Allows businesses to securely share information with selected suppliers, partners, customers, or other businesses.
9. **Company has stand-alone computer –** Computers that are not connected to company networks, such as a stand-alone workstation. For the purposes of this survey, a stand-alone computer may have Internet access.

Question 2b – In 2001, was there any type of wireless accessibility to this company's computer networks?

Wireless accessibility refers to the use of a device or system that will enable access to a network that isn't physically connected. For example, a cellular or digital phone, some personal digital assistants (PDAs), some laptop computers, thin client, broadband, etc.

Question 3a – In 2001, what types of computer system security technology did this company use?

Mark (X) the types of computer security technology the company used in 2001.

1. **Access control –** The protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities.
2. **Anti-virus software –** A utility that looks for viruses, alerts the user and quarantines any that are found.
3. **Biometrics –** Methods of generating authentication information for a person by digitizing measurements of a physical characteristic such as a fingerprint, a hand shape, a retinal pattern, a speech pattern (voice print), or handwriting.
4. **Digital certificates –** An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.
5. **Email logs/filters –** Email logs keep track of incoming/outgoing messages including the sender and the recipient. Filters are an automated method of searching the content of email for words, viruses or other misuse of computer resources.
6. **Encryption –** The translation of data into a format that requires a code to restore it to the original format. To read an encrypted file, you must have access to a secret key or password that allows you to decrypt it.
7. **Firewall –** A physical system or program designed to prevent unauthorized access to or from a private network. Firewalls can be implemented through hardware or software, or a combination of both. Firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.
8. **Intrusion detection system –** An intrusion detection system examines all inbound and outbound network activity and identifies suspicious patterns that may signal a network or system attack from someone attempting to break into or compromise a system.
9. **One-time password generators –** A "one-time password generator" is an authentication device such as a one-time token which randomly changes all or part of the user's password, typically every minute, so that the same password is never used more than once. This technique counters the threat of a replay attack that uses passwords captured by wiretapping or other means of hacking.
10. **Reusable passwords (change every 30 or 60 days, etc.) –** A simple authentication technique in which each password is used repeatedly for a period of time, typically 30, 60 or 90 days, to verify an identity.
11. **System administrative logs –** Logs which document details of access to computer systems, such as who logged in, which parts of the system were accessed, when the user logged in and out.

Question 3b – In 2001, how much did this company spend on security hardware/software for its computer networks and internal applications?

Security hardware/software refers to any hardware or software that is used specifically for computer security. It may be bundled or purchased separately, off-the-shelf or custom-designed. See the list in Question 3a for examples.

Question 3c – In 2001, did this company use short-term security services from a third party contractor for its computer security system?

"Short-term" security services refer to a third party contractor engaged for less than 6 months either in a part time or full time capacity specifically for security services. Note that the same individual may in fact be used for a whole year, however the tasks are defined in portions of a year. For example, the person was hired for 3 months for firewall services, 6 months for workstation virus integration, 3 months for point to point private virtual network services, and so forth.

Question 3d – In 2001, did this company use managed security services from a third party contractor for its computer system security?

"Managed security services" from a third party contractor include a variety of service options such as monitoring the security environment, managing a firewall and/or VPN, remote scanning and anti-virus/anti-vandal filtering, and so forth to protect online resources and to ensure safe, uninterrupted business operations.

Question 4a – Which statement best describes the status of any business continuity/disaster recovery programs for this company's computer systems at the end of 2001?

Mark (X) the box that describes the status of the company's business continuity/disaster recovery program at the end of 2001.

A business continuity/disaster recovery program is a plan that ensures that an organization can continue to operate after a disaster that would normally prevent it from doing so. For example, a dual system in a separate physical location or frequent back-up of files to a separate disk.

A disaster recovery program is the company's plan details how to respond to a computer system emergency. It includes procedures for reporting specific types of problems to designated personnel, ensuring the business community program is in place, repairing or replacing damaged systems, etc.

Question 4b – If a computer system business continuity/disaster recovery program was in place, was it tested in 2001?

Testing typically includes conducting a series of operations, checks or dry runs on the company's business continuity/disaster recovery program to ensure that it worked effectively and remained appropriate to the needs of the organization.

Section III – UNLICENSED COPYING OR USE OF SOFTWARE

Question 6a – In 2001, did this company experience any unlicensed copying or use of software which it developed or for which it holds the copyright?

"Unlicensed copying or use of software" refers to the unauthorized copying or use of software produced by this company for re-sale or developed by this company for internal use.

Section IV – TYPES OF COMPUTER SECURITY INCIDENTS

Questions 7a – 7d, Embezzlement

Question 7a – Did this company detect any incidents in which any computer was used to commit embezzlement against this company in 2001?

This question obtains information on whether the company experienced any computer security incidents resulting in embezzlement.

Question 7b – How many of these incidents of embezzlement resulted in monetary loss in 2001?

Monetary loss includes actual losses such as the value of stolen information, stolen or damaged property, forged financial documents, etc. It may also include the estimated value of downtime, income from lost sales, lost productivity, etc.

Question 7c – What was the monetary loss incurred in 2001 associated with these incidents (before any settlement proceeds or awards)?

We will provide instructions later.

Question 7d – Was any of the money or other things of value obtained in these incidents of embezzlement recovered in 2001?

We will provide instructions later.

Questions 8a – 8d, Fraud

Question 8a – Did this company detect any incidents in which any computer was used to commit fraud against this company in 2001?

This question obtains information on whether the company experienced any computer security incidents resulting in fraud.

Question 8b – How many of these incidents of fraud resulted in monetary loss in 2001?

Monetary loss includes actual losses such as the value of stolen information, stolen or damaged property, forged financial documents, etc. It may also include the estimated value of downtime, income from lost sales, lost productivity, etc.

Question 8c – What was the monetary loss incurred in 2001 associated with these incidents (before any settlement proceeds or awards)?

We will provide instructions later.

Question 8d – Was any of the money or other things of value obtained in these incidents of fraud recovered in 2001?

We will provide instructions later.

Questions 9a – 9c, Forgery or Theft of Proprietary Information

Question 9a – Did this company detect any incidents in which any computer was used to commit a forgery or theft of any proprietary information in 2001?

This question obtains information on whether the company experienced any computer security incidents resulting in forgery or theft of proprietary information.

Question 9b – Did any of these incidents of forgery or theft result in monetary loss in 2001?

Monetary loss includes actual losses such as the value of stolen information, stolen or damaged property, forged financial documents, etc. It may also include the estimated value of downtime, income from lost sales, lost productivity, etc.

Questions 10a – 10d, Denial of Service

Question 10a – Did this company detect any UNSUCCESSFUL attempts of denial of service to its Internet connection in 2001?

This question obtains information on whether the company experienced any computer security incidents that were **unsuccessful** in accomplishing denial of service to the company's computer system.

Item 10b – Did this company detect any SUCCESSFUL attempts of denial of service to its Internet connection in 2001?

This question obtains information on whether the company experienced a network or system attack from someone who **successfully** gained access to or compromised the company's computer system to commit a denial of service to its Internet conection.

Question 10d – Did any incidents of denial of service to its Internet connection result in monetary loss in 2001?

Monetary loss includes actual losses such as the value of stolen information, stolen or damaged property, forged financial documents, etc. It may also include the estimated value of downtime, income from lost sales, lost productivity, etc.

Questions 11a – 11d, Vandalism or Sabotage

Question 11a – Did this company detect any incidents in which any part of its computer networks was vandalized or sabotaged in 2001?

This question obtains information on whether the company experienced any computer security incidents resulting in vandalism or sabotage.

Question 11c – Did any of these incidents of vandalism or sabotage result in monetary loss in 2001?

Monetary loss includes actual losses such as the value of stolen information, stolen or damaged property, forged financial documents, etc. It may also include the estimated value of downtime, income from lost sales, lost productivity, etc.

Questions 12a – 12d, Computer Virus

Question 12a – Did this company detect any incidents in which a virus was DETECTED BUT NOT EXECUTED in 2001?

This question obtains information on whether the company experienced any computer security incidents that were **unsuccessful** in executing a computer virus to the company's computer system.

Question 12b – Did this company detect any incidents in which a virus was EXECUTED in any part of its computer networks in 2001?

This question obtains information on whether the company experienced a network or system attack from someone who **successfully** gained access to or compromised the company's computer system to execute a computer virus.

Question 12d – Did any of these viruses result in monetary loss in 2001?

Monetary loss includes actual losses such as the value of stolen information, stolen or damaged property, forged financial documents, etc. It may also include the estimated value of downtime, income from lost sales, lost productivity, etc.

Questions 13a – 13d, Other Computer Security Incidents

Question 13a – Did this company detect any other UNSUCCESSFUL, attempted computer security incidents in 2001?

This question obtains information on whether the company experienced any other **unsuccessful** network or system attacks to the company's computer system.

Question 13b – Did this company detect any other SUCCESSFUL computer security incidents in 2001?

This question obtains information on whether the company experienced a network or system attack from someone who **successfully** gained access to or compromised the company's computer system to commit other computer security incidents.

Question 13d – Did any of these other intrusions result in monetary loss in 2001?

Monetary loss includes actual losses such as the value of stolen information, stolen or damaged property, forged financial documents, etc. It may also include the estimated value of downtime, income from lost sales, lost productivity, etc.

Questions 14a – 14g, Total Losses and Settlements

Question 14d – What was the TOTAL monetary loss incurred in 2001 associated with all computer security incidents detected (before any settlement proceeds or awards)?

We will provide instructions later.

Question 14g – What was the TOTAL value of money or things of value RECOVERED in 2001 associated with all computer security incidents detected?

We will provide instructions later.

Section V – SPECIFIC INCIDENT INFORMATION

Question 15a – What was the single most significant computer security incident for this company in 2001?

Mark (X) only one. Refer to the definitions provided in Question 1 for categories 1–7.

Question 15c – Which elements of this company's computer networks were affected in this incident?

Mark (X) only one. Refer to the definitions provided in Question 2a for categories 1–9.

Question 15d – If this company had wireless accessibility to its computer network in 2001, was it used as means of intrusion in this incident?

Wireless accessibility refers to the use of a device or system that will enable access to a network that isn't physically connected. For example, a cellular or digital phone, some personal digital assistants (PDAs), some laptop computers, thin client, broadband, etc. If the company did not have wireless accessibility to its network, mark category 4, "Not applicable."

Question 15g – What was the monetary loss incurred in 2001 associated with this particular incident (before any settlement proceeds or awards)?

We will provide instructions later.

Question 16 – What was the relationship between the suspected offender and this company at the time of this incident?

Mark (X) only one. If there were multiple offenders, answer for the one viewed as the principal offender.

If the relationship between the suspected offender and this company has changed, e.g., employee was fired after the incident, indicate the relationship at the time the incident occurred.

4. Foreign competitor, foreign hacker, or other foreign entity - Refers to incidents caused by foreign entities. Indicate the country of the foreign entity, if known.

5. Hacker/cracker (no known association with this company) – Refers to an individual who tries to break the security of and gain access to someone else's system without being invited to do so. Also, for this category, such an individual has no known association with the company.

Question 17 – To whom was this incident reported?

Mark (X) all that apply.

4. **CERT® Coordination Center –** An organization that studies computer and network security in order to provide incident response services to victim of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.

5. **System Administration, Networks, and Security (SANS) Institute –** A cooperative research and education organization through which system administrators, security professionals, and network administrators share lessons learned and find solutions to challenges they face.

6. **Federal Computer Incident Response Center (FedCIRC) –** The central coordination and analysis facility dealing with computer related issues affecting the civilian agencies and departments of the Federal Government.

Question 19a – Which line of business most closely corresponds to this company's' primary activity in 2001?

Mark (X) only one. Mark the industry in which your company operated in 2001.

Question 19b – What were the total sales, receipts, and operating revenue (net of returns and allowances, and excise and sales taxes) for this company in 2001?

Report sales, operating receipts, and revenue at the end of the year for goods produced, distributed, or services provided. Include revenue from investments, rents, and royalties only if it is the principal business activity of the company. For example: finance, insurance, and real estate companies.

Include all operating receipts from taxable operations, as well as total revenue from tax-exempt activities (contributions, gifts, grants, etc.). Report revenues from customers outside the company including sales of products and services to other companies, individuals, U.S. Government agencies, and foreign customers. Include transfers to foreign subsidiaries.

Exclude domestic intra-enterprise transfers, sales by foreign subsidiaries, freight charges and excise taxes.

Question 19c – What was the total number of employees ON THIS COMPANY'S PAYROLL for the pay period which includes March 12, 2001?

Count EACH part-time employee as one.

Include:

- All full- and part-time employees on the payroll during the pay period including March 12, 2001.
- Salaried officers and executives of a corporation.
- Salaried members of a professional service organization or association (operating under State professional corporation statutes and filing a Federal corporate income tax return).
- Employees on paid sick leave, paid vacations and paid holidays.

Exclude:

- Contractors, purchased or managed services, professional or technical services.
- Proprietors or partners of an unincorporated company.
- Full-and part-time leased employees whose payroll was filed by an employee leasing company.
- Temporary staffing obtained from a staffing service.

Question 20 – Do the data you reported in this survey cover the calendar year 2001?

If category 2 is marked because the data reported are for a period other than calendar 2001, please enter the beginning and ending dates in the month and year boxes provided.

Question 21 – What was this company's operational status at the end of 2001?

Mark (X) the one category that best indicates the operational status of this company at the end of 2001. If category 4 or category 5 is marked, enter the month and year the action became effective. Also, if category 5 is marked, provide the name and address of the successor company.

CONTACT INFORMATION

Provide the name, title, telephone number, fax number, and e-mail address of the person to contact if we have questions regarding the information provided on this questionnaire.